UiO : Faculty of Law
University of Oslo

Biometrics and Banks in Finland from a Privacy Perspective

Candidate number: 8014

Submission deadline: 1.12.2013

Number of words: 17151

Table of Contents

1 Introduction

Biometrics has been coming into the awareness of public for a while. No longer it is a hypothetical or even infeasible technology from science fiction movies where machines can recognize and read people from their body parts, but actually it is coming not only to real life but one might even say to everyday life, some even expecting the biometrics to be the main stream of the information technology in coming years. Biometrics is an identification and authentication technology utilizing the unique characteristics of human bodies, such as fingerprint, iris, voice etc.[1] Identification and authentication of an individual is essential in both in practice as well as legally for it links and associates the data with the individuals themselves. Used correctly it is possible that biometrics would make the identification easier by increasing both the quality and speed of the process. Nevertheless the use of biometrics is not unambiguous and brings problems with it. These problems are unique in their nature since biometrics differs from other recognition systems, such as passwords, personal identification numbers (PINs) etc., due to the fact that biometrics are based on the uniqueness of individual human body; something you have naturally already. Unlike passwords, PINs or even signatures biometric characteristics are not dispensable. In case someone is able to present somebody else's biometrics as their own –there is nothing to do about it- it is not possible to change fingerprints, voice, veins etc. Too light use of biometrics, meaning the use without evaluating properly the possible disadvantages of biometrics, raises questions, issues and concerns about individual's data and privacy protection and fundamental rights. Nevertheless this uniqueness of characteristics causing the alarming issues is also the asset and strength of biometrics providing better privacy protection than the more traditional ways are currently providing.

Identification is extremely important in banks and its meaning cannot be highlighted enough. Identification has to be smooth and trustworthy so that banking can work in a pro-

[1] Liu (2010), p. 1, Yun (2003), p.84

per manner. In banks the identification often happens by presenting a document, which verifies the aspects of the identity. In many countries for example passports are accepted as one form of identification but more and more of banking activities are issued without human interaction. People are using ATMs, online banking, mobile banking etc. and in these means there is no one to physically inspect whether you are the person you are claiming to be or not. Other ways have had to come up. In ATM's consumers traditionally use a four-digit PIN code. This code is typed after the ATM has recognized the consumer's personal bankcard. In online banking a consumer registers himself for the service by setting up customer numbers and/or passwords to be verified. More than likely it goes without saying how absolutely necessary the correct and reliable verification is in these banking applications. However these systems are not solid and there are relatively simple and effortless ways to steal financial personal information of others. For example a criminal is able to steal your PIN at ATM by just posing as another customer in the line or the criminal might have set up a camera to capture the customers' PIN. In this work it is discussed whether the possible use of biometrics in banking application would increase the security in transactions or should banks abstain themselves from using biometrics due to the disadvantages and threats that biometrics may raise.

The purpose of this work is to by researching biometrics in the light of privacy and data protection to recognize the possible need to amend the legislation. The approach of this work is to research this need by analyzing the interaction between biometrics, privacy and banking and this leads to three sub-questions investigated in this research:

1. How are biometrics and privacy related to each other? Are biometric applications a bless or a threat to privacy protection?
2. What kind of privacy problems may biometric applications cause in banking? On the other hand what are the advantages and benefits of biometrics in relation to banking and privacy?
3. What would be the appropriate legal solution to these challenges?

At the early steps of this work I found a thesis made in Finland in 2006, which analyzed and considered very similar issues as this work.[2] The work also elaborated different biometric characteristics and their applications. However the author of the work, Kriikkula did not take a stance on whether biometrical devices should be used in banking or not, but still came into the same conclusion that the need for reform of legislation is urgent. It needs to be highlighted that Kriikkula made his work on 2006, seven years earlier than this work. There have been some minor changes in legislation, which are relating to the biometrics and online banking, for example the Act on Strong Identification and Electronic Signature came into force 2009. However the core of the problem, the Personal Data Act has not been changed yet. The same problems and lacks are still current.

So that the research questions could be answered they are dealt with different parts of the research. This research consists of six chapters the first one being the introduction.

In the second chapter the biometrics are presented. Some of the most common different techniques of biometrics, such as fingerprints, face recognition and iris recognition are explained. Also it is examined what biometrics is and what are the properties that need to be fulfilled so that characteristics can function as biometrics. This chapter is not about legal analyze but is necessary and relevant so that the rest of this research can be understood correctly. At the end of this chapter there is an evaluation about the most suitable biometric technology in banking applications.

The third chapter begins with the overview of banks and their tasks in the society. For an account of clearness some expressions and definitions used in this work are pointed out. Chapter three also elaborates bank security especially concentrating on the security problems in today's world. It is also analyzed how the biometrics can be used in banking and what kind of pros and cons biometric applications may cause to both banks and individuals. In addition a few biometric applications relevant to banks are presented.

---

[2] Kriikkula (2006)

The fourth chapter presents the legislation relevant to data protection and accordingly biometrics focusing especially on Finland's Personal Data Act, which is the legislation, applied when using biometrics for identification or authentication purposes in Finland. At the end of the chapter the problems and lacks of the current legislation situation are highlighted.

The last chapter before bibliography concludes this work by providing a short summary of this work, answers to the research questions and includes personal recommendations.

The main method used in this work is legal dogmatic. This means that the law what is now applicable is described and analyzed. However this work includes also some technical discussion when the different biometric technologies are elaborated. Thus it could be said that the scientific frame of this work is in legal informatics.

2 Biometrics

2.1 What is Biometrics?

Your voiceprint locks the door of your house, your iris is scanned at the airport, your face is automatically recognized at the casino (at least if you are a casino fraudster), you give your fingerprint to be filed onto your passport. These different applications are all using biometrics; in all these cases your body, your unique physical characters are working as a key to get an access to different services or used to automatically recognize you.[3] Biometrics is an automated recognition of an individual according to his or her physical, physiological or behavioral feature. The term derives from two separate words from ancient Greek: "bios" meaning the life and "metron" meaning measure. Biometric technology is thereby an automated measurement of physiological or behavioral characters to verify or recognize

[3] Grijpink (2005a), p. 139

the identity of a person. The emphasis is on the words "automated" and "person": "automated" highlights the technique of biometric authentication, which is done completely by machine.[4] Therefore for example the DNA identification is not, in general, considered to be biometric recognition technology since it still encompasses some manual work instead of being totally automated.[5] The second key word is "person" since biometrics is interested to recognize people as an individual moreover than for example linking persons to groups or connecting groups of people.[6] Biometric recognition technology is not determining who you really are, what your true identity is but to recognize you from all the other people.

Hence biometric authentication or identification is not based on what you remember, what you have or what you know (as are for example locks and keys, smart cards or numeric keypads), it is based on what you *are*.[7] It is based on your features, your skin, your eyes, your voice, what you physically are or how you behave. Biometrics types can be divided into two main, generic categories: to physiological and behavioral. Oxford Dictionary defines physiology to be "the branch of biology that deals with the normal functions of living organisms and their parts."[8] A physiological biometric is based on some physical trait which is assumed to be at least relatively unchanging; for example fingerprints, iris patterns, facial features and hand geometry. However also behavioral biometric can be based on physiological characteristics, for example our voice is influenced by physical characteristics of the diaphragm.[9] Behavioral biometric is anyhow something what is *learned* and involves the cognitive process that is not part of the physiological biometrics. Examples of behavioral biometrics could be for example signature or typing on a keyboard.

But if it is possible to use for purpose of biometrical recognition both something we are and something we have learned, could it be that everything made by a person could be use as

[4] Wayman et al. (2005), p.1
[5] Liu (2010), p. 27
[6] Wayman et al. (2005), p.2
[7] Boukhonine et al. (2005), p.941
[8] Oxford Dictionary (2013)
[9] Boukhonine et al. (2005), p. 941

biometrics? The problem with most of the behavioral biometrics is that they are not exquisite enough to provide reliable identification. So although in theory it would be possible to use any characteristics to biometric recognition, from the way we drive a car to your painting style, in practice it would not work. This is at the heart of biometrics: the trait has to be as unique as possible. Many behaviorals, such as car driving style, painting style or tapping, may be used for identification purposes but they are not reliable enough to be used in the real world biometric applications.[10] There are five qualities that the ideal biometric character would have: robustness, distinctiveness, availability, accessibility and acceptability.[11] Many behaviorals lack these qualities. Robustness refers to the degree the trait significantly changes over time; highly robust biometric does not change prominently over time.[12] Distinctiveness means the variation over the population, availability the extent to which the entire population has the measure, accessibility the degree of easiness to image the trait using electronic sensors and finally acceptability the amount people do not want to this measurement to be taken from them.[13] Different biometric have different qualities. For example iris does not change a lot over time but some people might find the scanning uncomfortable and are involuntary for the measurement. There is no "best biometric characteristic" but different evaluations have made some biometrics characteristics more appropriate than others. For example whether or not the characteristic is dependent on the specific application, the population and administration policy are influencing to the suitability of the use of biometric characteristic. [14] Later in this chapter some of the most used technologies are presented.

2.2 How Biometric Technologies Work?

[10] Yampolskiy and Govindaraju (2008), p. 83-84
[11] Wayman (2001)
[12] Liu (2010), p. 32
[13] Wayman et al. (2005), p. 3
[14] Ibid.

There are several steps before the physical or behavioral characteristics can be used as a way to identify or verify a person. Usually there is a pattern in which the following processes are involved: 1) obtaining the biometric sample of an individual, usually by using a scanner or camera 2) determining the biometric template from the biometric sample 3) saving this template for future reference 4) allowing access in the future in case there is a similarity between the presented biometric sample and its reference sample.[15] This is an authentication system in which it is determined whether the particular person is the person who she or he claims to be. The aim is not to determine who this person really is but moreover to know that this is the same person, a person with the same biometric information, no exact identity is concerned. In identification process on the other hand an individual's biometric information is captured to compare whether this information matches to a template stored in a database. Identification can be passive and even happen without the knowledge of individual. An example of this kind of passive identification would be a surveillance system in a casino where the camera captures face images of the customers. These pictures are passed to a computer and this computer tries to find a match from database. This database is made by the casino and contains pictures of the faces of the casino fraudsters. In this way the casino fraudsters are being identified passively and needed security actions can be conducted. On the other hand if the computer cannot find a match between the biometric information and database, accordingly the system does not then know the individual and the biometric information is deleted.[16] If in the biometric authentication the question would be*: is the person who she or he claims to be*, then in the biometric identification the corresponding issue would be: *who is this person*? While in identification systems the biometric information is always stored in the database controlled by custodian[17], in authentication systems it is possible that the biometric information is only in the hands of the owner. For example it could be a smart card where the biometric information is stored and the reader reads and compares the biometric template from the card, not from

[15] Buyn and Buyn (2013), p. 218. Coventry (2003)
[16] Boukhonine et al. (2005), p. 942-943
[17] Liu (2010), p. 35

database. However this is not usually the case since for back-up reasons in addition to portable media also a central database has been generally created.[18]

2.3 Different Technologies

There is no "best biometric". No superior characteristics exist that would have all the ideal five qualities mentioned in this work. There are pros and cons for every biometric characteristic and naturally for the technologies using different biometric characteristics too. What kind of technology should then be used? It all depends on what is wanted to achieve. One technology using biometric might be suitable for airports where it is used hundreds of times each and every day and is fast and easy to use. The other one is more appropriate to small offices, for example in embassies, where it is crucial that the number of accuracy level is as high as possible but the slowness and possible difficulties in use are not an issue. The choice of technology should not be only about cost-efficiency or accuracy level but also understanding the user's perspective and abilities to use the technology.

2.3.1 Fingerprints

For many of us the word biometric brings fingerprints into our minds and indeed it is one of the most used biometric technologies.[19] It is the oldest method, already used in 1986 for criminal identification[20] and nowadays different kinds of applications from different spheres of the world exploit fingerprints in their use. Not anymore only law enforcement agencies use it to identify criminals but also for example in civil applications fingerprints are used in border control and driver registration and in commercial applications in personal access protection and banking security.

---

[18] Liu (2010), p. 35
[19] Wayman et al. (2005), p. 21-30
[20] Yun (2003), p.86

Fingerprint refers to the pattern left by the friction ridges of a human finger. These ridges are flowing from one side to another non-continuously and form a unique pattern; discontinuity then gives a rise to feature points named minutiae and the pattern of flow gives rise to arches, whorls and loops.[21] There are three different ways to recognize fingerprints.[22] The minutia recognition is based on minutiae that are like small pixels constituting a picture of our fingerprint. Pattern-based algorithm uses both micro and macro features of the fingertip. Macro features are relatively large components such as loops. The third way, hybrid algorithm then exploits the best features of previously mentioned algorithms.

Fingerprint recognition is relatively easy to use in theory but in practice there are number of variables which may conspire the probability to capture image of fingerprint with a good quality.[23] For example the cleanliness of the scanning surface and precise position and attitude of the fingerprint while placing it to the surface may lower the accuracy level. Also impaired or damaged fingerprints may be difficult to verify.[24] However in general fingerprint recognition can achieve a relatively good accuracy level to both authentication and identification.[25] It is also cheap compared to many other biometric recognition technologies. A fingerprint scanner may even cost under 50$ while for example iris scanner can cost around 1000$.[26]

Spoofing is an attempt to trick the biometric system to believe that the biometric characteristic presented is a feature of an authorized user when truly it is not and fingerprint recognition systems are not free from spoofing either. Fake prints can be used in fingerprint

---

[21] Yun (2003)
[22] Boukhonine et al. (2005) p. 943-944
[23] Ashbourn (2000), p. 45-49
[24] Boukhonine et al. (2005), p. 943-944
[25] Yun (2003), p. 88
[26] Boukhonine (2005), p. 945

recognition system and some might require the cooperation of the authorized owner while in other cases only a digital image of a fingerprint might be enough to trick the system.[27]

2.3.2 Face Recognition

A facial recognition device takes a picture or video of a person and then sends the information to a computer, which compares the picture to the faces in database and tries to find a match. Face recognition is thus more focusing on recognizing the identity of an individual from a database while face verification concerns the authentication of a claimed identity.[28] The most beneficial use however would be on facial verification as it is easy to alter the face with mask, glasses, make-up etc.

The techniques of face recognition can be roughly divided into two groups[29]: In the first technique the device recognizes certain points of the face, which are less endangered to alteration, for example these characteristics could be the side of the nose and points at the eyes. Then the device is doing a geometrical relationship between these points and their locations and obtains the face recognition. The negative side of this approach is that all the other information than fiducial features are ignored. In the holistic approach the device processes the entire face image simultaneously and thus no information is disregarded. However such a device can be very vulnerable to all the external factors, such as brightness.[30] All in all several technologies such as 2D, 3D and infrared facial scans are in use.[31] Usually face recognition is passive and happens without the knowledge of an individual.

---

[27] Liu (2010), p. 47
[28] Wayman et al. (2005) p. 98
[29] Yun (2003), p. 85-86
[30] Ashbourn (2000), p. 56
[31] Liu (2010), p.50

Facial recognition is a bit problematic with its robustness, anyway. People change over time. Natural aging happens to all of us but for example due to the accidents or diseases some people's face may change substantially, even unrecognizable.

2.3.3 Iris Recognition

Iris is a muscle that regulates the size of the pupil in the eye controlling the amount of light that reaches the retina, thin layer of cells that lines the back of the eyeball. How light is reflected from the iris minutiae differs among individuals so the optical sensing suits well for recognition processes.[32] It has also been discovered that not only are the iris pattern unique to the individual but also the left and right irises are unique themselves.[33]

The uniqueness of the iris is one thing but capturing this uniqueness into the recognition processes is another. To capture one's iris the individual looks into the camera. Iris imaging requires a high quality camera; to get a reasbonable picture of the iris is not only about sufficient resolution and sharpness but also the contrast between the iris patterns has to be sufficient. All this has to happen as imperceptibly as possible without causing any harm or discomfort to the data subject. There are three main steps in iris matching[34]: the first step is to establish spatial correspondence between two iris signatures. In the second step the goodness of the match between two iris signatures are quantified. Lastly decision-making has to be done: are the two signatures deriving from the same physical iris or not?

Iris recognition is a relatively new and promising area for biometric recognition. Iris corresponds sufficiently well to the requirements of ideal biometric characteristics. Iris is robust: the patterns vary to little past childhood.[35] Naturally there is always a possibility that

---

[32] Wayman et al. (2005), p. 65
[33] Ashbourn (2000), p. 52
[34] Wayman et al. (2005), p. 79
[35] Ibid, p. 67

some disease would change the pattern but in general iris is both robust and distinctive. Acceptableness of the iris recognition might be a problem of some kind. Many people are very sensitive about their eyes and although the cameras are nowadays at a comfortable distance, still some people might feel the scanning inconvenient or intrusive.[36] For some individuals having for example a poor eyesight or disabled persons the use of iris scanners might cause difficulties when the camera needs to be aligning with the eye.

Iris scanning represents high accuracy for appropriate applications although it is not free from spoofing either. One can spoof the device by printing out an image of iris with a high quality. However fortunately it is possible to teach the biometric system to recognize a printed image.[37]

2.3.4 Vascular Pattern Recognition

In vascular pattern recognition, also called as vein pattern recognition, the vascular of a human body is used as an identification method. The palm vein sensor uses an infrared ray to reflect or transmit images of the user's palm. The sensor is able to capture the image of the palm despite the movement and position of the palm and the lightning of the near-infrared ray are controlled depending on the illumination around the sensor.[38]

Vascular pattern recognition has many advantages on its side: the scanning happens without any contact to sensing surface so for example compared to fingerprinting it is much more hygiene so the dirtiness of the surface cannot have an influence on the accuracy level.[39] Also it is undisputable that a healthy human needs to have blood vessels and the vein patterns are highly complex in the hand area, which advocates the principle of uniqueness

---

[36] Boukhonine (2005), p. 950
[37] Boukhonine (2005), p. 950
[38] Watanabi et al. (2005), p. 1
[39] Ibid.

and universality.[40] Vascular pattern recognition does not either have any association to most of people and thus is not easily related to criminal investigation. Vascular pattern recognition devices are mostly used in East-Asian countries, for example in Japan, where they are more widely accepted among the users than fingerprint devices.[41] Since vascular patterns are also internal and unexposed it is almost impossible to duplicate or forge them making the spoofing difficult.[42] However the accuracy level of vascular pattern recognition is still doubtful.[43]

2.3.5 Voice Recognition

In voice recognition the identification or authentication of a person transpires by characteristic of the speakers voice. Voice is both a behavioral and physiological biometric thus for example the shape of throat and mouth are physically influencing to the voice but on the other hand voice pitch and speaking style are behavioral patterns. Voice is a natural technique for recognition since we use our voice every day in the most ordinary situations, which makes its use familiar and safe and acceptable for user's perspective. Hence it is not surprising that voice recognition is one of the earliest biometric examples in commercially available products.[44]

Voice recognition system has two main steps.[45] In the enrollment phase the speaker's voice is recorded and in the verification phase this sample is compared to the voice given in the first phase. It needs to be highlighted that it is not only the sound of the voice influencing to the correct matching but also physical construction of an individual's vocal chords, vocal

---

[40] Hartung (2012), p. 44
[41] Ibid.
[42] Watanabi et al. (2005), p. 1
[43] Liu (2010), p. 54
[44] Ashbourn (2000), p. 59
[45] Boukhonine (2005), p. 951-952

tract, palate, teeth and sinuses affect the dynamics of the speech.[46] However the voice is not expected to be distinctive enough to permit identification from large database.[47] The problem is that voice can vary due to for example aging or cold. Also some people may experience problems with the accuracy due to the way they speak or the nature of their voice.[48] Many of the characteristics of voice are impossible to produce artificially, which decreases the number of spoofs. This does not remove the possibility to spoof the device based on playback.[49] It has also been researched that even a simple voice conversion system had been able to break down all the voice recognizers considered in the research.[50]

2.4 Biometric Technologies and Banking Applications

All the technologies presented in the previous chapter do have their own advantages and disadvantages. Some of the biometric technologies, like iris recognition, are giving better accuracy level than others, like face recognition, but on the other hand they are more slow and more difficult to use, some might even consider them to be intrusive. However there is no unnecessary biometric technology; every biometric characteristic has its own pros and cons like technologies exploiting them. Some characteristics suit well for other applications and are useless for the others. What biometric characteristic and technology should be used then depends on all what is wanted to achieve.

In banking environment there are at least two factors, *customers* and the *essential need for security*, which are making the banking environment different from other environments exploiting biometrics, for example companies that use biometrics in their access control, and which do raise special concerns and issues when considering the possible use of bio-

[46] Ashbourn (2000), p. 59
[47] Liu (2010), p. 52
[48] Ibid.
[49] Boukhonine et al. (2005), p. 951
[50] Kinnunen et al. (2012)

metrics and which technology would be the most suitable. These factors need to be taken into account when deciding the most convenient biometric characteristics exploited in banking applications:

1. Customers: Banks are designed to serve every citizen. They provide their services not to some limited, inside groups but oppositely to mass market.[51] Accordingly the applications, whether exploiting biometrics or not, have to be designed in a way that as many people as possible are capable of using them. This culminates especially to two demands that have to be met:

    - Technology: Banking applications cannot be too complicated to use but they have to be made as customer friendly as possible. This might cut out some biometric characteristics. For example iris recognition is at the time being very sensitive about the position and distance and might thus result to false rejection.[52] As simple use of the devices as possible is particularly critical for elder and disabled people.

    - Robustness: Since the customer base of banks is voluminous, the robustness of biometrics is crucial; updating biometric characteristics to databases continuously would require too much both time and effort from banks and customers. Thus it is beneficial for banks point of view that the biometric characteristic would change as little as possible over time. This makes the use of

[51]This applies to both online banking and traditional banking services; for example there was a comprehensive debate really recently in Finland when one of the biggest banks refused to give online banking username to its client having an immigration background. The bank defended its decision on grounds of lack of regular incomes. The majority of the people critiziced heavily bank's manner of an approach arguing that online banking username is a basic banking service and should be provided for every natural person. See for example Repo (2013) and Pettersson (2013)

[52] In false rejection the technology using biometrics fails to recognize the authorized person and rejects she or he as an impostor. Compare to false acceptance in which the system incorrectly authorizes a non-authorized person by matching incorrectly the biometric characteristic input with the one in template.

some biometric characteristics if not impossible, at least unsuitable. For example the use of face recognition could be problematic considering the natural aging, which is extra problematic among youngsters who grow continuously and whose facial features can change comparatively fast. Applications exploiting voice recognition would face the same complications concerning for example the pubertal change of the human voice mutation.

- Availability: Since the customer of the bank can essentially be anybody, the availability of the biometric characteristics is fundamental; the application should be possible to be used by everybody. Thus for example the use of fingerprints might be problematic. Fingerprints are relatively sensitive biometric characteristic since for example due to certain kind of harsh work the person's fingerprint might have been worned away.

2. Essential need for security. The need for highly secure recognition is extremely important in banking environment and this creates pressure especially to the accuracy level of biometric applications. In banking environment it does not matter how fast or convenient the device is if the false rejection and false acceptance rates are high; bank activities cannot work if the banks do not recognize their customers accurately. This is derived from the fact that if the system is not secure, the threat that someone exploits the system is great and its consequences are severe since the attacker can gain financial benefit otherwise than in many other entities. For example university library might use biometrics to recognize whether a particular customer has the right to access to the library and lend books or not; whether he or she is the student of the particular university or not. The consequences of possible misuse of this kind of system are not even comparable to ones in banking. When considering the most suitable biometric technology in banking the importance has to be in accuracy. This excludes many technologies instantaneously, i.e. behavioral biometrics are not secure enough.

Biometric technologies do offer a broad range of applications that could be exploited in banking. However, as noted above, the technology should be suitable for mass market and also be as secure as possible. These requirements are cutting out most of the biometric characteristics. At the time being fingerprint technology is the most used technology among banks using biometric technology. Approximately 48% among these banks use fingerprints in different activities and the next mostly used biometric technologies are finger vein pattern and voice recognition.[53] However these characteristics and technologies exploiting them all have their weak points, as already presented and they are not ideal for banking either. Nevertheless there is a direct need for workable biometric technology also in banking environment. One of the solutions could be to combine different biometric technologies together. For example professor Busch, analyzed the future biometric method in banking in the following way: "In the concrete case of biometric online banking tamper-proof biometric sensors are essential […] In future we can expect a "biometric secoder" to be used that authenticates transactions by combining fingerprint recognition with finger vein recognition."[54]

On the other hand banks are not traditionally the pioneers or early adopters of new technology. They need to be especially sure about the acceptance levels and robustness attained before adapting new kind of technology.

3 Biometrics and Banks

3.1 Overview of the Banks and Evolvement of Banks

Finnish law does not define the term bank in a way that it could be reasonable to use the definition in this work. According to the Finnish Act on Credit Institutions a deposit bank is a credit institution, which may accept deposits and other repayable funds from the public

[53] Hosseini & Mohammadi (2012), p. 9154
[54] Dapp (2012), p. 12

and a deposit bank may be a limited company, a co-operative or a savings bank.[55] Basically deposit banks are credit institutions having a trade name to deposit banking activity. On the other hand other than a deposit bank, the Bank of Finland or the Nordic Investment Bank may not use the term "bank" in its name unless it its indisputable that the term does not misleadingly refer to the activity of a deposit bank.[56] This definition might exclude for example some investment services. In this work the term bank should be understood in the broadest possible sense. Also the term "financial transactions" correspondingly is used in a wide context in this work meaning transfers of information together with payment activities and account activity.[57] In addition in this work the term "bank card" refers to any kind of cards used in financial performances, i.e. credit cards, debit cards and ATM cards.

E-banking may be used as a synonym for online banking but in here the scope of online banking is tighter than e-banking. The term online banking refers in this work to a system, which allows the customers of a financial institution to access their bank accounts and access the information regarding services and products provided by their bank.[58] These performances go via Internet, not for example through telephone network. The device used in online banking usually is a computer or mobile telephone. In Finland most of the people use online bank services to pay the bills and to check their account balances and recent transactions. It is not common for example to apply for a mortgage online. The trend seems to be that people are willing to do their daily bank affairs online but do not see arduous to transact business in banking branch in case of more infrequent matters. E-banking on the other hand indicates "the umbrella term for the process by which a customer may perform banking transactions electronically"[59] and hence refers also for example to ATMs and telephone banking.

---

[55] Act on Credit Institutions, Chapter 1(9)
[56] Ibid, Chapter 2(21)
[57] The Department of Treasury (2005), p. 2
[58] Ahmad & Hariri (2012), p.1
[59] FinCen (2000), p. 25

If you research biometric applications in banking in Europe you can notice relatively promptly that the amount of the applications using biometrical characteristics is very limited. Biometric applications have not penetrated to the bank and payment organization worlds yet as one could have expect. In this work the biometric applications in banking refers to the applications in online banking services and in ATMs albeit biometric applications can be also used in many other ways in the financial industry as already stated previously in this work. However some kind of limitation is necessary due to the limited scope of this work and online banking and ATMs are services concerning the majority of the people, unlike for example employee screening, which would also be possible by exploiting biometrics and is linked to the banking world. Banks in Europe are still commonly trusting to more traditional security certificates, like passwords and usernames than to biometric authentication.[60] There is a great diversity of biometric applications that financial industry could exploit if they would choose to do so, from network access control to ATM verifications and the most optimistc ones even believe that it is possible to create services that are not even existing yet but what only biometrics could enable.[61]

Banks and financial industry has generally been an area where changes go on slowly. Already in Ancient Egypt and Greece there were institutions that took in gold and other valuables in exchange for charges and for example the first municipal bank in the whole world, "Taula de Cambi" has its roots already in the 14th century.[62] The very substance of the banks has not changed from these times. On one hand all the banks are to some degree identical considering their core functions to be the same: safekeeping money, making of payments, making of loans, making of investments et cetera. On the other hand banks diverse from each other's. They might be disparate in their very nature, in degree of speciali-

[60] There are some exceptions for this. For example Poland's BPS SA Bank installed the first biometric cash machine in Warsaw in 2010. See for example Biometric Technology Today (2010)
[61] Biometric Technology Today (2005), p. 9
[62] Anttila (1996), p. 50

zation, in legal status and in place they occupy in the system to which they belong like such as investment banks, retail banks, online banks and commercial banks.[63]

The evolvement of IT has also left its marks to traditionally slowly changing banking although banks may have had fears towards technology that might have been unreliable. Financial industry is information intensive business and IT has enabled the rapid transmission of information, which has correspondingly grew the amount of information.[64] It could be said that e-banking has extended the already existing banks and also created new banks.[65] Roughly divided IT has caused three major changes in the banking world[66]:

1) IT has expanded the existing products into new markets and started the era of mass market banking
2) Alternative distribution channels were opened up, for example credit cards appeared
3) IT enabled the cash dispenser experiments, leading to ATMs

Owing to these changes e-banking adapts to customer's life effortlessly. People do not have to plan their schedule according to the office hours anymore but services of the banks are available for everybody at anytime. Information technology's influence has not only added the demands and requirements of the customers but it has also changed the activity of banks from their own point of view and also for their own good. Banks are now closer to customers than ever and many features and functions are nowadays automatically processed and do not need any human interaction, which has decreased the expenses of the banks since less staff and less physical branches are needed nowadays. Without e-banking for example paying bills would have required the customer to go the bank with his or her bill, stand in the queue to get to the desk, be served by bank's employee who then would have

[63] Scott (1914), p. 2-6
[64] Anttila (1996), p.80
[65] Omariba et al. (2012), p. 433
[66] Liao et al. (1999), p. 64

taken the money from the customer and pay the bill for him or her. Instead the same customer can now go online anywhere and anytime he or she prefers and come to the same final result with much less effort and time via telecommunications network.

Nevertheless online banking has not been adapted so strongly among customers than most banks were wishing for.[67] Many customers are worried about the safety and privacy issues. In principle all the companies have the same risks as banks but the characteristics of banking and banking regulation give them their own unique nuance that might be crucial to the customers.[68]

3.2 Bank Security

Evolvement of online banking has changed the nature of the risks involved in banking environment. While everything is nowadays online and in a virtual world it is not the most extensive concern to worry, in the Western world at least, that someone would walk into the bank or break in and try to rob it. Traditional threats are coming more and more irrelevant and new, technological risks have to be taken into account and taken seriously.

Online banking does not create risks only to its customers but also to banks themselves. With risk in this work is meant a threat of loss, fall or other unbeneficial action either expected or unexpected.[69] With the evolvement of IT, banks now have to bear the risks of credit, interest rate, liquidity, price, foreign exchange and reputation.[70] All the same there are other actors posed in risk too. Governments have to take into account the antitrust laws and concern the reserve requirements of banks and the consumer protection laws concerning electronic transfer of money.[71] Businesses are having their concerns of their security

[67] Calisir & Gumussoy (2008), p.215
[68] Anttila (1996), p. 37
[69] Ibid.
[70] Sarma & Singh (2010), p. 70
[71] Yang (1997), p. 4

of money and possible savings in time and financial charges[72]. This work however focuses on the various types of risks that individuals have to face while using online-banking. The main concerns are security of transactions and loss of anonymity of a customer. Anonymity of an online-banking customer can be threaten if the attacker gets the information of amount of transaction, date and time of transaction or/and the name of the merchant.[73] According to Omariba et al. (2012) there are eight main attacks that e-banking can suffer and which can have an unwanted effect to the privacy and security of a customer[74]:

1) Social engineering in which a technical expertise is not even required but in which an attacker poses as for example a customer service and tries to trick the customer to reveal some sensitive information.
2) Port scanners are used to steal information with the aim of finding an active port and then the plan of attack can be committed.
3) Packet sniffers gather data that is passed through network
4) Password cracking
5) Trojans can secretly connect and send confidential information
6) Denials of service attacks overloads the server and render it useless. While server is down the attacker can have an access to database or a user's system
7) Server bugs
8) In super user exploits attacker gains the control of the system as being an administrator of the system

All these different methods can threat the privacy of a customer of online-banking. The technological threats and risks of online-banking should not be underestimated but banks

[72] Ibid.
[73] Omariba et al. (2012)
[74] Ibid, (2012), pp. 440-442

should instead take them into serious consideration to secure customer's safe use of virtual banking.

In addition to online-banking this work focuses on ATMs. Customers using ATMs also have to take into account some security issues. There are several mechanisms how an attacker can violate customer's privacy in ATMs. Mostly known frauds are committed by using cameras to record the customer's PIN or simply just standing behind the customer and pretending to be the next the customer on line. There is no point to start introducing all the possible methods where the sensitive data used in ATM can be stolen or misplaced considering that these methods are rapid and ever changing in their nature.[75] Even the most imaginative methods have been committed, for example criminals have installed devices to record the sound from the keyboard when customers have typed their PIN-code. Different digits have different sound.[76]

3.2.1 Bank Security in Finland

Although the banks themselves might see their security systems to be adequate the customers may see it differently. The following numbers and information are originated from Statistics Finland's report concerning the use of information and communication technologies from year 2010.[77] According to this report every nine out of ten Finnish people uses the Internet, three out of four use Internet daily and half of the citizens several times a day. In a digital world Finnish people are most worried about the misuse of their bankcards and children's access to inappropriate websites. When it comes to the misuse of bankcards nearly half of the people are worried at some level, every fifth Finn is extremely worried and every fourth answerer had give up thoughts to buy some services or goods from Internet due to the information security concerns.

---

[75] Omariba et al. (2012), p. 440
[76] Lee (2004), p.14
[77] Statistics Finland (2010)

On the other hand in Finland people trust online banking services, which are provided by Finnish banks. Only five to six percent of the answerers had abandoned thoughts to use online banking due to the information security concerns and when every nine out of then Finns use Internet at least occasionally this number can be considered to be satisfyingly small.

Despite the fact that Finnish people trust virtual banking environment, misuse of bank cards happen in Finland and the number has been growing in recent years. The payment offenses are reported to the police with the following designation of crime: counterfeiting, aggravated counterfeiting, petty counterfeiting or preparation of counterfeiting.[78] Naturally the payment offenses may include also other manners than bankcards, like for example cheques. However the use of cheques and especially their misuse is negligible in Finland. The following table describes the number of payment offences, essentially misuse of bankcards, reported to the police in last years[79]:

Year	2007	2008	2009	2010	2011	2012
Number of Payment Offenses	3784	3835	5166	4517	5670	6463

As the total number of crimes reported to the police in 2012 was 425 421[80], the portion of bankcard frauds is approximately 1,5 percent. The number may seem to be small but it should not be considered to be inconsequential at all. For comparison the number of rapes was 1020[81], for percent's only 0,2.

[78] The Criminal Code of Finland, Chapter 37
[79] Police of Finland (2013)
[80] Statistics Finland (2012)
[81] Ibid. (2012)

From these statistics we can conclude that the current situation is not ideal in Finland. Payment offenses exist in Finland and even in a growing number. In addition it is extremely crucial to remember that for example identity thefts are not included here in number of payment offenses. Since there is no such a crime as an identity theft in Finland the keep of statistics happens with several disparate designation of crimes. However identity thefts and crimes relating to it cannot be excluded from crimes relating to online banking; false identities are often used for offenses related to financial interests. As it has been analyzed in this work, biometric applications in banking might enhance the security but for it to be workable, the legislation should be appropriate and support both the users and service providers.

All these security threats raise the importance of privacy protection. It is now more relevant than ever to pay attention to the recognition of the customers. Back in those days where people went physically into the branches of banks it was uncomplicated to ask the customer to present document of their identity. It is in the foundation of secure bank service that bank recognizes its customers and in online-banking this recognition has to happen electronically but still as reliably as traditionally. Essentially there are two ways how the security of banks can be enhanced: by technology improvements and by better security policy, which can be highly pressured by the legislation. Biometrical applications can improve the level of accuracy of identification and authentication. In chapter 3.3 the different biometric applications in banking environment and their pros and cons are analyzed.

3.3 Biometric Applications in Banks

Biometrics is used successfully in many spheres of life, like for example in law enforcement and in physical access. However the use of biometrical characteristics is still in its infancy in banking environment despite the fact that the appropriate technology has existed for years already and the need for safer banking environment is constant. Banks do not use biometric applications in Finland; there are no banking devices exploiting biometrical cha-

racteristics. Both the online banking and ATM security systems trust on traditional passwords and username manners of approach. The representative from one of the biggest banks in Finland has announced that current security systems are adequate and there is no need for massive changes and even if there would be, these changes would not change the manner of an approach of biometrics: "in future other means of identification will be more usable solutions than biometric identification and OP-Group sees the current data protection legislation to be sufficient and the reform of legislation unnecessary since the biometric devices will not be applicable".[82]

In this chapter it will be discussed how different biometrical applications can be used in the banking environment. The required technology, implementation across the banking environment and the pros and cons of these applications will be elaborated.

3.3.1 ATMs

The use of biometric applications in banking environment has so far concentrated especially on ATMs, which is reasonable since the great deal of the banking crimes in developed countries are crimes committed by abusing the ATMs. These kinds of crimes not only concern the customers but also bank operators themselves and have so become a nationwide issue.[83] ATM with the use of biometrics is not a new idea though. Despite the fact that commonly in Europe and in the USA ATM security is still based on PIN-codes or other similar passwords, the use of biometric characteristics are relatively popular outside these areas. There are banks in Latin America, Asia, Africa and in the Middle East where biometric-enabled ATMs are used daily. Some countries are also rolling it out at the time being, like for example India.

---

[82] Ministry of Transport and Communication (2013) ,p. 39 author's own translation
[83] Onyesolu & Ezeani (2012), p. 68

Generally ATM, which uses biometrical characteristics, works with three stages. In the first stage the biometric sample, for example fingerprint, is created and then stored to bank's branch, network provider or only into the customer's physical card. In the second stage ATM reads the bankcard and in the final stage the customer types the password, PIN-code or gets the biometrical characteristic scanned. Most of the ATMs use magnetic strip and personal identification number to support each other's.[84] However in ATM using biometrics, the individual's unique characteristics such as voice or vascular patterns are used in verification. Instead of typing PIN the customer is required to produce a trace similar to the sample created for the database. The ATM then forwards the information to a host processor, which leads the request to customer's financial institution. If a customer is withdrawing cash for example after the funds have been transferred, the ATM receives a code approving the withdrawal, which gives it green light to disburse.[85]

The most common biometrical characteristic used in ATMs are fingerprints where the customer presses his or her fingerprint against the scanner after the ATM has identified customer's card.[86] On the other hand the security and reliability of ATMs using fingerprints have been questioned since they can be relatively easily lifted and replicated.[87] Many ATMs for example in Japan and Brazil are using vein pattern recognition instead where infrared light passes the palm or finger and detects the unique pattern of customer's microvein.

The newest concept is to have an authentication system in ATMs, which does not require any physical cards. For instance Fujitsu has revealed a biometric system in which a customer scans his or her palm and the device reads the unique pattern of the veins of the palm. After this the customer inputs his or her PIN and birth date and in this way gets an access to the bank account. The idea behind this device is that if people would lose their bankcards

[84] Lohiya (2012), p. 2
[85] Orr & Bielski (2000), p. 4
[86] Onyesolu & Ezeani (2012), p. 71
[87] Hartung (2012), p. 60

and passports or other identity cards due to for example natural disaster like earthquake, they would still be able to access their accounts.[88]

The use of biometrics in ATMs offers an alternative option for traditional PIN-codes and passwords. Some think that with the help of biometrics ATM security can be strengthened[89] and others claim that biometric characteristics are one of the lasts frontiers of individual privacy.[90]

3.3.2 Online Banking

Banks use different kinds of programs and software in their online banking. The significance of safe online banking environment cannot be emphasized excessively. Without satisfactory safety level and the customer's trust online banking could not operate. However the legal rules applied for online banking do not constitute a uniform field of law or legislation on its own. Moreover the general principles from established fields of laws apply also to online banking. The rules and principles specifically concerning online banking are in their nature mainly contract law and consumer protection.[91] However depending on the issue, different laws and rules have to be taken into account. For example in the process of designing the online bank system in addition to contract law and consumer protection also intellectual property rights, international private law and data protection law have to be taken into a consideration.

In many countries it has been considered that single password authentication is not enough to safeguard availability, confidential integrity, accountability and non-repudiation and

---

[88] Fujitsu (2012a)
[89] Boukhonine et al. (2005), p. 957
[90] Gunn (2010)
[91] Wuolijoki (2005), p. 237

two-step authentication is preferred instead[92]. In two-step authentication there are two separate levels to verify the customer. So instead the online banking program asking only username and password it also requires for example single use one-time password in addition. Single use one-time password is valid only one login session or transaction after which it will not be used again.

Online banking applications exploiting biometrical characteristics however do not use traditional passwords but rather use the biometrical characteristics for authentication. Biometrics can be used in online banking in several ways and there is no established policy. Instead different banks have seen appropriate to adopt applications that may differ even quite notably from each other's. Few examples of possible applications will be presented.

One of the ways is that banks can sell biometric security kit for their private customers, which includes the biometric device and the self-enrolment and authentication application software. The biometric device can be for example a desktop biometric fingerprint reader. Biometric template can be combined with the bankcard info or e.g. birthdate info and stored on the local biometric device system. In case the authentication is precise, the authentication server of bank authorizes transaction via bank's data center executing the customers' accounts.[93]

There are also new applications coming into the market, which do not require extra devices at all. OpenSezMe is a mobile phone app developed by VoiceKey, which uses the user's voice as a key to get an access to personal data on mobile phone. The program is based on the customer's voice classifiers, which is established when the customer speaks a random phrase three times. The classifiers are stored in to the customer's mobile phone and the phrase is sent to the VoiceKey server. It is in the server where the verification process takes place and if the classifiers match, the server transmits a confidence score back to the

[92] Venkatraman (2008), p. 420
[93] Fujitsu (2012b)

customer's mobile phone. While the program is still used for marketing aid, the ambition is that the app could replace PIN-codes in financial transactions.[94]

Also facial recognition has been tried to use together with passwords in banking environment. The problem seems to be that customer's are not ready to invest to the devices and cheap low-resolution web cameras have such a poor quality that the false acceptance rate varies between ten and fifteen percent, which is very high on both biometrics and banking environment.[95] With proper devices, the numbers would be different.

It seems to be that the amount of different kinds of biometric devices and manners of an approach, which can be exploited in online banking, are unlimited. Notwithstanding biometric applications have not been managed to come into the knowledge and use of the public in online banking environment and only 10% of the world's banks use biometrics in online banking and in Europe only 9%[96]

3.3.3 Pros and Cons of Biometric Applications in Banking Environment

Several arguments on behalf of the use of biometrics in e-banking can be presented. There is no doubt about the fact that there are benefits of biometric supported devices also in banking environment. This chapter focuses to elaborate both the benefits and the risks of these devices and the balance between them.

3.3.3.1 Advantages

---

[94] Hudson (2013)
[95] SecurityInfoWatch.com (2007)
[96] Hosseini & Mohammadi (2012), p. 9156-9157

The first major benefit of biometric devices in banking environment is that they provide *strong authentication.*[97] This is in the very heart of biometrics and concerns all the devices no matter from what sphere of the world; biometrics are traits of an individual; they are much harder to copy, share or steal than i.e. PIN-codes, which makes the forging more demanding.[98] This advantage is being emphasized in virtual banking where the priority is to provide a secure and safe environment where customers can perform their transactions. Compared to PINs, usernames and passwords the advantage of biometrics is that they identify the customer themselves instead of i.e. bankcard, which means that the owner of biometric characteristic will most probably be the authorized customer.[99]

The second benefit is the *consumer convenience*.[100] The customer's do not have to strain their memory anymore. In these days people have to remember several series of numbers from mobile phone's PIN to online banking usernames and from wife's birthday to workplace's burglar alarm's security code. We are persistently straining our brains with all this information. Too much remembering and thinking can be exhausting. Many people have a half dozen credit-, debit- and bankcards in their wallets and all they have different PIN-codes and so that the PINs and passwords are working effectively they should be as complex as it is possible to remember. Many people also have several online banking usernames in different banks and different banks have different styles to constitute their usernames and passwords. If biometrics is used instead of PINs there is not so much to remember anymore. People might feel that doing business in ATMs or in online banking using biometrics is much less stressful as the key to get the access to their account is something what they *are*, not what they *know*. Some people write down their PIN-codes, usernames and passwords used in banking environment so that they would not have to recall these identifi-

[97] Bhosale (2012), p. 11
[98] Ahmad & Hariri (2012), p.1
[99] Boukhonine et al. (2005), p. 939
[100] Buyn (2013), p. 219

ers. However the dilemma is that these cheat sheets can be stolen, misplaced or left at home for example.[101] The same issue does not concern biometric characteristics.

The third benefit is the *savings*. Although the start-up of biometric devices can be costly the use of biometrics for example in ATMs can cut costs that are caused by the use of traditional ATMs. These hidden costs can be for example card personalization, delivery, management, re-issuance, helpdesk and re-issuance.[102] It needs to be also mentioned that the prices for biometric devices are perpetually coming down making it more economical for bank to adopt biometrical security systems.[103]

3.3.3.2 Disadvantages

3.3.3.2.1 Counterarguments for Advantages

There are counterarguments for the benefits; savings and consumer convenience. It all depends on which aspect the issues are analyzed.

Despite the advantages resulting from memory relief, customers might feel that the ATMs or online banks using biometrics are technologically difficult to use and it always takes time before people are used to new technology. This difficulty might concern especially seniors and disabled persons. Also some customers might feel the new technology to be too intrusive, coming too close to the "real me".

If the banks decide to start using the biometric devices, in the beginning the investments can be rather outstanding despite the fact that prices are coming down perpetually. Especially devices recognizing fingerprints are nowadays at very reasonable prices. Howe-

---

[101] Sarma & Singh (2010), p. 73
[102] Bhosale (2012), p. 11
[103] Wayman et al. (2005), p. 57

ver not only are the devices themselves necessary but also the software to enroll and compare the biometric characteristics are required. Banks should also prepare themselves to other expenses; as already mentioned it might take some time before the customers get used to biometric devices and before that they might need some extra help and guidance. Also the staff needs to educate themselves.

Uses of biometrical devices are often justified, in banking environment like in any other sphere, with the increased safety level. However the use of biometrics in banking applications raises many questions from data and privacy protection. And it is not only the actual use of biometrics but moreover the issues where and how the banks would create, compare and link the data of the customers. One of the overwhelming uncertainties concerns the storage. Liu (2010) presents several questions where privacy and security issues are involved in this regard:

- What kind of biometric information is stored?
- What are the security measures taken to protect the data from unauthorized use?
- Is the biometric information stored together with other personal information?
- Does the system prevent tampering and how?

Although the strong authentication is a considerable advantage all the same biometrics cannot provide exhaustive certainty in verifying the legal holder of a biometric characteristic, as biometric devices do not produce the *exact* same template on every incident.[104] It is also possible to spoof biometric devices and the consequences of misuse of biometrical characteristics might be much more far-reaching than what could be for example in case someones PIN-code is stolen. One of these far-reaching consequences and the biggest threat of use of biometrics is an identity theft.

[104] Grijpink (2001), p.155

3.3.3.2.2 Threat of an Identity theft

Imagine a world where biometric characteristics would be used in every sphere of life. No matter whether you would go to a buss, café, cinema, workplace or bank, biometrical tracks would work as a key to get the access and they would work alone, without smartcards or other physical appliances. Then imagine that someone would steal your biometrical characteristics, for example your fingerprint. What could you do?

Identity theft has not been criminalized in Finland and thus there is no definition of it in the legislation. It is not illegal according to Finnish law to pretend to be someone else than who you really are.[105] Identity theft in this work means: "abuse of personal data or documents with the purpose of using somebody else's identity and performing illegal acts, for example abuse of the person's bank account or other securities".[106] In online environment *"identity"* can be, addition to personal data, any identifier which is used to distinguish entities from each other's or to indicate that: 1) the possessor of the identifier is the one he or she claims to be 2) the possessor of the identifier has the right to get access to the information or service, which the real possessor of the identifier is entitled to.[107] In banking environment this could mean i.e. the access to a bank account. Indeed banking and identity thefts are closely connected, many identity thefts occurring through individual's private financial information, i.e.:

- Theft and unauthorized use of someone else's bank card
- Skimming bank card's account numbers from magnetic stripe

[105] According to the Finnish Penal Code 28(1) in theft the perpetrator appropriates movable property from the possession of another. However in identity theft it is not required that the identity is taken away but it can also be used in conjunction with the legitimate person. The perpetrator moreover copy's the information from his/her own use also.
[106] Hosseini & Mohammadi (2012), p. 9153
[107] Ministry of Interior (2010), p.48

- Misuse of information from credit reports[108]

Also phising is used to commit an identity theft. In phising for example the customer of the bank gets an e-mail, which tricks the customer to hand over their personal information, i.e. the username and password of online banking system or bank card details to criminals themselves. However there is not much biometrics could do to stop the phising happening since the customers are voluntarily turning over their personal information although being spoofed. Banks should emphasize to their customers that banks do not themselves inquire the usernames or passwords of customers via e-mails or live chats.

Biometrics can be used as means to combat against identity thefts. Some biometric devices can authenticate the customer's identity positively but are making the access resources by stealing for fraudsters challenging, i.e. iris scanning.[109] What if the breach would happen nevertheless? If the world would be like described in the beginning of this chapter the individual whose biometric characteristic was stolen would be in an truly inconvenient position. If the imposter would have managed to steal his or her biometric characteristic and the biometric technology products alone would be used to authenticate the people, the imposter could anytime authenticate falsely. On the other hand if the individual would want to prevent this happening she/he would need to close herself/himself out of the systems using biometrical characteristics decisively.

The fear is that people are not taking the possibility of identity theft seriously enough and that biometrical devices are not given visibility in this light. In Europe the awareness of identity theft is limited and often only those who have suffered from one and their family, closest friends and colleagues seem to be aware of the threat.[110]

---

[108] The Department of Treasury (2005), p. 7-8
[109] Zegiorgis (2002), p. 1
[110] Wayman et al. (2005), p. 351

4 Data Protection and Biometrics in Finland

4.1 Commonly about Privacy

In earlier times the communities were small and the personal information was preserved among the family members, members of the community, neighbors and friends. If some information were spread usually it was a hearsay, something that was heard by gossiping or storytelling. Traditionally the concern with privacy was not a problem with shearing the information but moreover it has been the concern of state big brothering us, classical opposition between an individual citizen and the state. The fear of government intruding our lives and having too much knowledge and even control about what we are doing, where and when.[111]

Nowadays, mostly due to the rapid evolvement of information technology, dimensions of privacy are broader than before and its meaning and significance cannot be overstated. Although privacy is a basic civil and constitutional right, it is a concept that does not exist only for its legal recognition; it exists by virtue of habits of life appropriate to its existence, like security for example.[112] It sustains human dignity and has an importance in our psychological, sociological, economical and political spheres of life.

So the concept of privacy has evolved and changed during the time. However the core of the definition can still be understood in the same way as decades before. Privacy is about people's ability to decide what and what kind of information about them is revealed to others; it is "claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others*".*[113] However the nuances and extent of it have a different nature nowadays than before and how you define privacy and

---

[111] See for example George Orwell's novel Nineteen Eighty-Four where people are under complete surveillance, which results to world almost without any love, creativity or other virtues
[112] Gross (1967), p. 36
[113] Westin (1967), p.7

its dynamics depends on how you analyze the situation and what point of view you take.[114] Data protection on the other hand is the set of norms aiming to protect privacy, at some extent at least, by regulating the processing of data concerning data subject.[115]

Privacy protection is a crucial part if biometric technologies are wanted to exploit and develop in a responsible manner.

4.2 Finland's First Steps in Privacy Protection

Finland is part of the European Union and its privacy protection has evolved hand in hand with the European legal framework. Privacy is a core human value provided by many international treaties such as United Nations Declaration of Human Rights in article 12 and the International Covenant on Civil and Political Rights in article 17.

The European Convention on Human Rights reflects the values of the modern world and provides a list of guaranteed rights. One of these rights is article 8 providing everyone's right to respect for his private life without interference by public authority. The article provides a broad interpretation and also biometric data has been considered to fall under article 8 in the S and Marper v. UK [2008] ECHR 1581 case:

S, being a minor at the time being, and Marper were arrested and charged with crimes of attempted robbery and harassment. However S was acquitted and Marper's chargers were dropped. The police had in both cases taken applicants' fingerprints and DNA samples and both of them asked the police to destroy their biometric data but the police refused to do it

---

[114] See for example Bygrave's Privacy and Data Protection in an International Perspective (2010) or Margulis' Three Theories of Privacy: An Overview (2011) for more detailed analyze about the definition of privacy

[115] Data Protection however should not be only see as a set of norms safeguarding privacy but also as a fundamental right, protected by i.e. Charter of Fundamental Rights of the European Union, art. 8.

arguing that the samples and profiles had been stored on basis of a law authorizing, retention being without time limit. Applicants argued that these provisions violated art. 8 of the ECHR retention being an interference with their private life and that this retention could not been justified by art. 8(2) allowing interference in case it is in accordance with law, meets legitimate aim or is necessary in a democratic society. The UK government argued that the information retained was not interference of private life as the information was considered to be neutral and even if the retention would go under art. 8 the effects of retention were not serious enough to constitute interference and accordingly breach of art. 8.

The Court disagreed with UK's government and found a breach of art. 8(1). It emphasized that private life is a broad term and is not capable for exhaustive definition as it covers "the physical and psychological integrity of a person".[116] The Court analyzed fingerprints and DNA profiles separately but came into the same conclusion with both data. With regards to DNA profiles the Court emphasized in its reasoning that person's health is an important element of private life and samples taken contained sensitive information about an individual, for example about health and the "retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned."[117] Court indicated also that fingerprint records constitute personal data and retention of them without the consent of individuals cannot be held to be neutral or insignificant as fingerprints may themselves raise private-life concerns and constitute an interference with the right to respect for private life.

The Court did not find any justifications in favor of UK government and found that the blanket and indiscriminate nature of retention of persons suspected but not convicted fails

[116] Case of S. and Marper v. UK, European Court of Human Rights 1, par. 66
[117] Ibid. par. 73

to strike a fair balance and was disproportionate and amounted for unjustified interference with the private life resulting a violation of art.8 of the Convention.[118]

Finland signed the named Convention on 1989 and ratified it a year later and accordingly it has to see biometric characteristics being part of individual's private life as the Court ruled.

In 1970's the number of personal data registers increased and the data protection started to draw attention in Finland as well. For example the Ministry of Justice set up a working party in 1971 to discuss about this new set of problems.[119]

Next meaningful step in Finland's data protection history was the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (from now on Convention 108) was drawn up in 1981 in Strasbourg. Finland signed and ratified it in 1991. Convention 108 is the only legally binding international instrument in data protection and its objective is to strengthen data protection. It sets out the minimum standards for protecting the individuals against abuses accompanied by the collection and processing of personal data.

In 1999 the Personal Data Act replaced the Personal Data File Act and was drafted because the requirements of the Data Protection Directive had to be met. The purpose of the Personal Data Act is to protect the private life and other basic rights safeguarding right to privacy while processing personal data[120] and includes the provisions that Data Protection Directive and Convention No. 108 on Data Protection oblige.

---

[118] Case of S. and Marper v. UK, European Court of Human Rights 1, . par. 125-126
[119] Konstari (1992), p.4
[120] Personal Data Act, Chapter 1(1)

There is no special legislation for biometrics in Finland. The Personal Data Act works as a general law and also regulates the use of biometrics but the biometrics has not either been excluded from the Act on Strong Electronic Identification and Electronic Signatures. [121]

4.3 Personal Data Act

According to the Constitution of Finland everyone's privacy shall be guaranteed and more detailed provisions of personal data shall be laid down by an Act.[122] Unless other provided, as a general rule a person has the right to control and administer his or her own personal data and decide on processing of it.[123] The collection and use of biometric data in Finland have to meet the requirements of Personal Data Act.

Does Personal Data Act then protect biometrical data? According to the Personal Data Act personal data is: "any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household"[124] The question here is what can constitute an identifiable characteristic. It is apparent that raw biometric data is personal data in the sense of Personal Data Act. Biometrical data is in its basic character related to personal characteristics, it is always applying to a particular individual. It is not necessary to know the exact name of the person so that the definition "personal data" can be used; moreover it is the data what makes the identification possible.[125]

Nevertheless according to the Data Protection Directive whether a person is identifiable or not depends on the reasonableness; the controller or any other person has to use all the *reasonable* means to identify the person in question.[126] So for example the fingerprints that we

---

[121] Act on Strong Electronic Identification and Electronic Signatures 617/2009
[122] The Constitution of Finland, Chapter 10
[123] Finland's Ministry of Interior (2010), p. 27
[124] Personal Data Act, Chapter 1 (3§)
[125] Hert (2005), p. 13
[126] Data Protection Directive, preamble 26

have left to the glass in a restaurant do not constitute a personal data in the sense of Personal Data Act; it is not reasonable to expect that someone would come and collect these tracks and try to identify us from them.

On the other hand Personal Data Act does not concern the personal data *per se* but furthermore *processing* the personal data. Processing of personal data is the collection, recording, organization, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data[127] and there are certain conditions that have to be fulfilled so that the processing would be lawful. The processing has to be appropriate, justified and defined before the collection.[128] The personal data must not be used otherwise.[129] The Personal Data Act accordingly regulates the processing of biometrical data.

The Personal Data Act sets out the general rules and provisions on the processing of personal data. The most crucial issues in the light of biometrics are ones concerning consent, proportionality, registration, storage, supervision and control. These rules and their wording are presented here in a more detailed way and their frailties and complexities when adapting them to biometrics are analyzed in chapter 4.5.

The personal data processed must be accurate and necessary to fulfill the purpose of processing according to paragraph 9 of Personal Data Act. This principle is one of the most essential since people have to have the right to be evaluated according to the correct and error-free data. Electronic authentication, including also the use and need of biometrics in this connection, should always be assessed by this requirement. Only data what is necessary for the purpose of processing may be collected and stored and therefore in cases where the use of biometric information would seen possible and necessary, the Personal Data Act requires to clarify the possible alternatives and their risks and effects. The prin-

---

[127] Personal Data Act, Chapter 1(3§)
[128] Ibid, Chapter 2 (5§)
[129] Ibid, Chapter 2 (7§)

ciple of necessity is not met incase there are other adequate, more appropriate and better privacy enhanced methods possible to use. The data collected and stored data shall be used only for the defined purposes and the purpose has to be defined in advance.

The personal data shall be processed only if the data subject has unambiguously consented to the same. However there are some exceptions to this, for example if the processing is necessary to perform a contract, is necessary for data subject's vital interests or there is a relevant connection between the data subject and operations of the controller, the data subject being a client or member.[130] According to the paragraph 24 of the Personal Data Act the controller has to see that the data subject can have information about the processing of the personal data; who collects the data, to what purposes the data is collected and where the data is transferred. The data subject also has the right to access and inspect the data on himself/herself and to get erroneous data corrected.

According to paragraph 32 of the Personal Data Act the controller has the obligation to secure the personal data against unauthorized access, accidental or unlawful destruction, disclosure or other unlawful processing by both technical and organizational measures. According to the same paragraph these means mean for example the associated costs, quality and quantity, age of the data and significance of the processing to the protection of privacy. The principle of protecting data apply to all stages; gathering, storage, use, registration and so on.

The Data Protection Ombudsman works as a supervisor on the processing of personal data providing direction and guidance. The controller has a duty to inform the Data Protection Ombudsman about the automated processing of personal data by sending a description of the file, which indicates the name and address of the controller, the purpose of processing

[130] Personal Data Act, Chapter 2 (8§)

the personal data, a description of data subjects, the regular destinations of disclosed data and the principles in accordance to which the data file has been secured.[131]

These rules and principles are the most relevant and at the same time the most problematic in processing of biometrical data. However it is decisive to acknowledge that Personal Data Act also governs other principles, like for example the processing of a personal identity number, although they are not presented here.

4.4 Act on Strong Electronic Identification and Electronic Signatures

Act on Strong Electronic Identification and Electronic Signatures (from here on ASEIES) is not a specific act of regulating biometrics. However it is necessary to mention it in this work since it does not exclude biometrics explicitly either. The object of the ASEIES is to promote the strong electronic identification and to provide basic rules for the supply of services without forgetting the data protection requirements. Additionally the determination of ASEIES is that legislation would not unnecessarily interfere or discriminate the formation of online contracts only due to their electronic form but moreover would enable the use of electronic signatures and goods and services related to it.[132] Therefore in the heart of ASEIES is the strong electronic identification, which is the identification of a natural person by an electronic method using at least two of three alternatives:

Password or something else that the identification device holder knows
Chip card or something else that the identification device holder has in his or her possession
Fingerprint or some other characteristic identifying the device holder[133]

---

[131] Personal Data Act, Chapters 7 (32§) and 2 (10§)
[132] Finland's Ministry of Interior (2010), p. 41
[133] ASEIES, chapter 1, 2§

It is characteristic to the strong identification that the identification device and its use are always, eventually, combined with person's real identity. This despite the fact that service provider using strong electronic identification device would not be informed of the actual personal information in other words there would be a so-called anonymous user.[134] The main rule is that the initial identification shall be done in person.[135]

Although ASEIES is more specific than Personal Data Act and might in some cases at least concern biometrics, it is not drafted to deal with the very basic problems of biometrics and privacy and thus cannot answer the possible need for specific regulation especially when the ASEIES does converse on in which cases the service requires strong electronic identification and in which cases not..[136]

4.5 Complexities with the Current Legislation

This chapter focuses to analyze whether there are any special privacy problems concerning biometrics, in which the current legislation is not answering accordingly. Biometrics is a special way to authenticate or identify a person in sense that it uses body parts in recognition process. Is it relevant or is there any significance on fact that unique characteristics are used as identifier or verifier? In this chapter it is presumed that the individual's body-related characteristics used in biometrics are unique although it has been questioned whether for example the fingerprints' uniqueness is just merely an assumption without absolute certainty.[137] Some grievances, that might become apparent if the current legislation is adopted also for the biometric applications, are analyzed.

---

[134] Government Bill 36/2009
[135] ASEIES, chapter 3 17§
[136] Ministry of the Interior (2010), p. 40
[137] See for example Cole (2000) and Stoney (1997)

4.5.1 Consent

The Personal Data Act regulates the general prerequisites for processing. Controller's obligation's regarding storage of personal data and its processing have been regulated accurately. Biometric data is no different than any other personal data; in some cases it can be gathered without the knowledge or permission of an individual and accordingly biometrics can be used for tracking individuals without notification. The concern is that biometric systems are capable to recognize individuals based on publicly appreciable characteristics and link this information with data about time and place of the observation. This threat is however more relevant to some biometric characteristics than others. For example we leave our fingerprints all the time to all over the places: to the glass from which you drank in the restaurant, to a door in which you opened to get into the grocery shop, to a book, which you groped at the library. However it is not reasonable or even rational to think that someone would use these traces to cause harm. On the other the security camera does not ask consent to take a picture of individual's face posing a great privacy risk resulting "biological" surveillance.[138] There have been advocates on both sides; those who commentate the benefits of facial-recognition to be much greater than the privacy issues[139] and those who see a whole list of arguments against its use and adoption: "automatic face recognition in public places […] should be outlawed. The dangers outweigh the benefits […] The potential for abuse is astronomical".[140]

After all the legislation should make certain that biometric data should be processed *only* with the consent of data subject. This would eliminate the threat of legally storing and processing biometric characteristics without the data subject's authorization.[141] The threat of lose of anonymity is actual when dealing with biometrics in purpose of authentication or identification and should not be underrated. The problem might be concrete for example in

---

[138] Liu (2010), p.87
[139] McCoy (2002), p. 471
[140] Agre (2003)
[141] Finland's Ministry of Transport and Communications (2003b)

facial recognition happening without the consent of data subject. If the processing and storing of biometric characteristics would happen only with the consent of data subject, the risk of someone losing their right to be anonymous would not be prejudiced on the grounds that identification or authentication without permission of data subject would not be legal no longer. This is the most crucial deficiency in the current legislation, which would allow, if the certain conditions are fulfilled, also the storage and process of biometric data without consent.[142]

Whether the threat that banks would gather biometric data without the consent of the data subject is relevant or not, is hard to evaluate. In principle it is possible that banks would i.e. take photos without permission of their customers doing businesses in bank branches to identify possible misusers. Howbeit this work concentrates especially e-banking applications and in these applications especially fingerprints and vein recognition are technologies used, which are challenging, vein pattern even impossible to gather without the consent or approval of the data subject. The trust of the customers is in the core of banking and it would seem to be irrelevant to be afraid of banks collecting biometric characteristics without customers' permission. Banks are using biometrics in online-banking to enhance the security and make customers' life easier and banking activities quicker, which eases both customers and banks themselves. On the other hand it is not the legislator's task to evaluate whether something is likely going to happen or not. No matter how unlikely or irrelevant it might sound that banks would collect biometric information without consent, it is anyway possible and it should be made illegitimate.

4.5.2 Too much information?

The general prerequisites for processing include the principles of necessity, accuracy and

[142] See for example Chapter 2, §8 (5) of the Personal Data Act under which the processing is legal if there is a relevant connection between the data subject and operations of the controller, based on the data subject being client or member of the controller

proportionality. The data collected should be adequate and relevant; no erroneous, incomplete or obsolete data should be processed. The data should not exceed the purposes for which it has been collected but moreover be necessary for the declared purpose of the processing. The concern is whether biometric systems will gather too much information about the individuals and thus would violate these principles.

On the other hand some argue that the use of biometrics would enhance the privacy protection since having a biometrical characteristics is enough, in addition you do not need any other information, such as race, age or gender or address, telephone number or name.[143] This is true. The uniqueness of the biometrics ensures that no additional information is needed. However the problem is that biometrics are containing too much information as such. For example from iris it is possible to detect some diseases and it is even possible to detect from a fingerprint the possible drug use or smoking because of secretions, skin oils and dead cells.[144] This leads to a fear that examination of biometric data, which might have been gathered only for authentication purposes, can help to identify the individual if so wanted. The principle of necessity is accordingly extremely important in biometrics; if there are other adequate, appropriate and more secure methods that can be used, the necessity requirement is not fulfilled. The use of biometrics should not be an end in itself but moreover only appropriate choice remaining.

Does biometric information then contain too much information so that it could legitimately be used in banking? It is clear that the safety of online banking is not foolproof at the moment in Finland. Misuses happen, hacking to bank accounts is relatively easy. Traditional usernames, passwords or four digit PINs do not provide the safety level needed. Is biometrics on the other hand "too much"? Does it contain too much information for the purpose of recognizing the customer in banking activities? And even if the necessity requirement would be fulfilled, can the banks be trusted or would the customers be in fear that banks

[143] See for example Boukhonine et al. p.963
[144] Hazarika et al. (2010)

utilizing biometrics would try to sell or trade the biometric data collected from the customers? The problem would occur for example in case where the banks would collect biometric information for their customer identification and then sell or trade this information to insurance company who would then be possibly able to gather health-related data from biometric information and get to know your possible disorders, which would then increase your insurance rates. Banks should refrain to transfer biometric information to other entities.

4.5.3 Supervision and Control

Next problem relates to the supervision and control of those controllers' that have biometric data in their hands. The controller has a duty to draw up a description of the personal data file, which indicates the name and address of controller, the purpose of processing the personal data and a description of the group of data subjects, security principles illustrating how the personal data is secured and the regular destinations of disclosed data.[145] This description of the personal data file shall then be send to the Data Protection Ombudsman.[146] The registration and storage of biometric characteristics should be held as secured as possible due to the their delicate nature and thus the controller should have an obligation to notify about the storage of biometric characteristics to the Data Protection Ombudsman. As the controller is already bound to send the description of the personal data file, this document could be extended to include also a section indicating the biometric information and its characteristics recorded.[147] These would make the supervision of controllers who are handling biometric data easier and accessible. Also it would enable to supervise these controllers' independently, which could raise the security level. Current requirements for the data included in the description of the personal data file are not sufficient to protect the biometric data's data subject.

---

[145] The Personal Data Act, Chapter 2, §10
[146] Ibid, Chapter 8, §36
[147] Finland's Ministry of Transport and Communications (2003b), p.54

4.5.4 Registration and Storage

Biometric characteristic can be used to identify the individual *per se.* It is very different in its nature compared to for example passwords or usernames, which do not indicate the data subject's identity. So that this identification or authentication would even be possible sample of biometric characteristic has to be registered and stored somewhere so that the comparison with the original sample and sample given in the moment of identification can happen.

The storage of biometric data should also be given additional consideration and the core question is whether biometric data should be allowed to store and register as such or should a method, which makes the generation of original feature inaccessible, be required. The personal data file issue is not a problem by itself but it is possible that the file ends up in the wrong hands due to i.e. hacking or the controller is in fraudulent mind. If the biometric characteristics would be stored and registered as such and the file would end up in the wrong hands, data subject's fingerprints, facial features, patterns of their veins or corresponding might be perhaps possible to copy and then distribute without any control. Sharing constitutes a problem in networked environment where templates can easily be linked together which makes it possible to perform cross matching and create a collection of an individual's information.[148] The basic rule in here should be that data from a certain zone cannot be automatically used in another, but moreover biometric applications need clear boundaries.[149] On the other hand technically it would be possible to store and register the biometric characteristic in a way that would make it impossible to figure or lead the original biometric characteristic.

The current legislation does not take a stance on issue in which form the biometric data should be registered and stored by any means. One solution could be for example that the

---

[148] Kevenaar et al. (2005), p.1
[149] Grijpink (2001), p.158

presumption would be that biometric data should always be registered and stored so that the original physical characteristic would not be possible to find out. However with a data subject's expressed and undisputable consent, biometric data could be registered and stored as such. This would both highlight individual's responsibility in decision-making and give more space to service providers to execute their services. However it can be argued whether an average individual with basic understanding of data and privacy issues and biometrics would be capable of doing such decisions.

Banks should abstain to store the biometric data to their own databases if there is a possibility to do so. The level of intrusion to privacy, when using biometrics, depends mainly about the method of biometrics selected and the storage of the biometric information. Especially in case of using the biometrics in ATMs banks should store the biometric information only to customer's own card instead of storing a copy of the code in a separate database. This would enhance the level of privacy since if the card would get lost or stolen only the authorized user would be able to use it. Also if the data were to be stored only in customer's card instead of bank's database, biometric information would be safe from possible hackers and distribution or trading.

4.5.5 Punishments

Since the biometric data is more sensible than traditional personal data, the causes from abuse of it should be more severe. According to the chapter 38 of Criminal Code of Finland and its section 9 a person who intentionally or grossly negligently processes personal data in violation of the provision of Personal Data Act and violates the privacy of the data subject causing damage or significant inconvenience shall be sentenced for committing a data protection offence to a fine or imprisonment for at most one year. The biometric characteristic is very different from its nature than other "traditional" personal data due to its uniqueness and exclusiveness. These features are making the threat of a loss of anonymity more severe; in case someone would lose their anonymity due to the misuse of their biometrical characteristics the loss of anonymity could also be permanent and constant. Biometric characteristics cannot be changed. Public authority should not only regulate the abu-

se of biometrical data to be punishable but also make the punishment harsher than what is regulated from the data protection offence.

4.5.6 Identity theft

The final concern is the scenario of an identity theft and as already mentioned in this work, Finland's criminal code does not criminalize identity theft *per se*. Biometric characteristics are not dispensable like for example passwords and PINs are. In case some would manage to commit an biometric identity theft, the only choice would withdraw the user from the system[150] as "once someone steals your biometric, it remains stolen for life; there is no getting back to a secure situation".[151]

The use of biometrics in authentication and verification sets some preconditions for the effective regulation. The main reason for the need of the more specific regulation is the permanence and uniqueness of the biometric characteristics; biometric characteristic is a permanent part of the individual and an individual can be recognized from this characteristic.

Two main reasons can be seen for the need for regulation:[152]

1) The protection of private life and the protection of the rights of an individual and
2) To safeguard the functionality and equality of commercial services

Finland's current legislation does not sufficiently take into account the characteristics of biometrics. There is a lack of legal clarity, which is a threat to both service providers and users. The current legislation does not give clear directions for service providers and it is challenging for them to assess where and when biometric identification or verification can

[150] Liu (2010), p. 100
[151] Schneier (1999)
[152] Finland's Ministry of Transport and Communications (2003a), p. 52

be used and how the data collected should be processed. Also the citizens' right to privacy is under a risk if more and more biometric identification based services are landing to Finland[153] and privacy and data protection requirements are not taken into account adequately.

4.6 What kind of Privacy Issues Banks should take into Consideration in case of Adapting Biometric Technology?

The current legislation does not provide clear rules for banks what they should take into consideration in case they want to adapt biometric technology in their activities. In this chapter I try to elaborate these different phases. Some of them could be guided directly from the legislation, others the banks should be capable to evaluate independently.

1. Is biometrics really required? Could there be some other techniques or alternatives, which could be adapted leading to the same final result? Banks should not adapt biometrics without proper justifications but there should always be strong arguments behalf of it. Are the possible privacy threats in right proportion with bank's business benefits?

2. When selecting the appropriate biometric technology banks should not only examine the costs and efficiency but also consider what biometric characteristic would be the least privacy abusive and how the technology and design of the application could on the other hand enhance the privacy. Banks should, to some point at least, also be committed to follow the advances happening in technology and be ready to change their applications in case technology with better privacy protection would be revealed.

[153] For example some gyms have already adopted biometrical applications for verification of customers in Finland

3. Banks should only gather the biometric information with customer's consent and also at the same time provide information why the data is collected, who is collecting it, where it is used, in addition to the bank does someone else have access to it, how the consent can be cancelled and possible time limits for both the use and store of the data.

4. Banks should primarily look to abstain themselves to create database of customers' biometric data but instead register and store it so that only the customer, the data subject would have the data in his or her hands, i.e. in case of ATMs store the data only to the bank card. In any case the registration and storage of biometric characteristic should happen in a way that it would be impossible to figure or read the original characteristic and banks should be accountable for the data, which it has collected.

5. In case a bank would adapt biometric technology it should still also offer other means for identification/verification, biometric system should not be the only option. This would protect the customers who do not want to use their biometric data for banking purposes and those who cannot use the system due to for example some disability from discrimination.

6. Banks should always be ready to give their customers information about their data and correct it incase of an error. Both of these should happen in a reasonable time and also manner.

5 Conclusion

At the beginning of this work I presented three sub-questions to be researched in this work. These questions were how biometrics and privacy are related to each other, what are the pros and cons of biometrics in banking environment and how legislation should answer to these challenges.

My prognosis for this work was very biometric optimistic. With my knowledge at the time I thought that biometrical applications in banking should be adapted also to Finland and even with "the idea the sooner the better". I was confident that the pros of biometrics would be overwhelming compared to the cons.

Biometrics and privacy really relate to each other's. On one hand the use of biometrics can enhance the privacy; it may give stronger security for example to banking accounts. On the other hand the use of biometrics can weaken data subject's privacy. The use of biometrics in light of data protection is not simple. There are several steps and levels where the intrusion to one's privacy may occur; in gathering, storage et cetera.

Still I think that the problem is not the biometrics *per se*. The use of biometric devices in banking would more than probably enhance the security and would decrease the number of payment offenses. Although in Finland there has not been much discussion about the security and safety of online banking, some think that it is only because nothing has luckily happened and that the threat is current and real. Online banking systems or especially ATMs are not as solid or without having any holes as people might think. For example Mikko Hyppönen, the Chief Research Officer for computer security company F-Secure estimated that Finland has only been lucky when bigger online banking attacks have not happened yet.[154] So something has to be done so that users' safety banking actions are also secured and protected in the future. Banks cannot trust to their security systems only on the grounds that they have been working in the history relatively well. The problem is that the evolvement of security systems is an ongoing race with the abusers. There are always people who are trying to find the loopholes of the security systems continuously.

Although becoming aware of the advantages of biometrics and their potential in virtual banking due to this work, I do not believe that biometrics is the right answer for the lacks

[154] Ollila (2013)

and inadequacies of banking systems. I find two main reasons for this: both legislation and users' knowledge.

Before the biometric applications can be used and they can reach their full potential the legal framework has to be in order. As presented in chapter 4.5 there are several lacks in the current legislation, which would need to be revised before the Personal Data Act is suitable for regulating biometrics and devices exploiting them. The most urgent lacks and needs are especially the following[155]:

1) Criminalization of unauthorized biometric identification
2) The use of biometric data only with the express and explicit consent of data subject
3) Extension of the description of personal data file; indication of biometric characteristic
4) The prohibition to store the biometrical characteristic *as such*

Before these changes have been made, the use of biometric application should be considered extremely carefully or even superior; to abstain completely. Personally I think the most appropriate approach would be to extent the current Data Privacy Act. This solution would be fast and easy since the framework with its established authorities already exist. A new code would be burdensome alternative and would take too much time as the need to change the legislation has already taken too long.[156]

The knowledge of users is another problem. Most of the people do not understand or even care about the privacy issues before they face some problems themselves or their neighbour becomes the victim. Biometrics is something really new in Finland and is not part of people's every day life and it would be unreasonable to expect that these people would under-

---

[155] Ministry of Transport and Communications (2003b)
[156] As mentioned in the Introduction, Kriikkula (2006) found similar gaps and lacks in the legislation already in year 2006.

stand the nature of biometrics. The risk would be that people would not care about the threats of biometrics and would start eagerly use the devices due to their user friendliness but would not realize the core problem of biometrics: *once you lose it, you cannot get it back*.

6 Table of Reference

Legislation and Other Legal Texts

Finland

Act on Credit Institutions (121/2007)

Act on Strong Electronic Identification and Electronic Signatures (617/2009) Unofficial English translation available on:
http://www.finlex.fi/en/laki/kaannokset/2009/en20090617.pdf (last access on: 31.10.2013)

The Constitution of Finland, 11 June 1999 (731/1999, amendments up to 1112 / 2011 included) Unofficial English translation available online:
http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf (last access on 27.11.2013)

The Criminal Code of Finland (39/1889, amendments up to 927/2012 included) Unofficial English translation available online:
http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf (last access on 31.10.2013)

The Personal Data Act (523/1999). Unofficial English translation available online: http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf (last access on: 31.10.2013)

Finland's Ministry of Interior (2010): "Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma)" Työryhmän loppuraportti. Sisäinen turvallisuus. Sisäasianministeriön julkaisuja 32/2010

Government Bill (2009): "Hallitksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista ja siihen liittyviksi laeiksi" 36/2009 vp.

Available online: http://www.finlex.fi/fi/esitykset/he/2009/20090036.pdf (last access on 11.11.2013)

Ministry of Transport and Communications (2003a): "Lausuntopyyntö" Dnro LVM 1609/30/2003 Available online: http://80.248.162.134/oliver/upl527-Lausuntokooste.pdf (last access on 4.11.2013)

Ministry of Transport and Communications (2003b): "Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve" Liikenne- ja viestintäministeriön julkaisuja 44/2003. Helsinki 2003

European Union

Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks and amending Directive 2002/58/EC

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.1.2012 (COM(2012)0011-C7-0025/2012-2012/0011(COD)

Council of Europe

European Convention on Human Rights and Fundamental Freedoms (1950)

Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (1981)

United Nations General Assembly

The International Covenant on Civil and Political Rights 6 December 1966, United Nations, Treaty Series, vol. 999

Court Decisions

S and Marper v. United Kingdom (GC) no.30562/04 and 30566/04, ECHR, (4 December 2008)

Literature

Afolabi, A.O & Adigun, A.A (2012): "Development of Crypto-Biometric E-Banking System" International Journal of Engineering and Technology Volume 2 No. 11, November, 2012. Available online: http://iet-journals.org/archive/2012/nov_vol_2_no_11/298199135667618.pdf (last access 29.10.2013)

Agre, P. (2003) "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places", 10 September, 2003. Available online: http://polaris.gseis.ucla.edu/pagre/ bar-code.html (last access on 25.11.2013)

Ahmad, D.T. and Hariri, M. (2012): "User Acceptance of Biometrics in E-banking to improve Security" Business Management Dynamics Vol.2, No.1, Jul 2012 pp.01-04

Anttila, T. (1996): "Pankki, riskit ja sääntely: oikeustieteellinen tutkimus mahdollisuuksista sääntelyllä hallita pankin riskejä" Lakimiesliiton Kustannus, Helsinki 1996

Ashbourn, A., (2000): “Biometrics: “Advanced Identity Verification. The Complete Guide ” Springer-Verlag London Limited 2000

Bhosale, S.T. & Sawant, B.S. (2012): “Security in E-Banking via Card Less Biometric ATMs” International Journal of Advanced Technology & Engineering Research. Vol. 2, Issue 4, July 2012

Boukhonine, S., Krotov V., Rupert B. (2005): “Future Security Approaches and Biometrics”, Communications of the Association for Information Systems. Vol.16, Art. 48

Byun S. and Buyn S. (2013) “Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters”. Behaviour and Information Technology, 32: 3, 217-230

Calisir, F. and Gumussoy, C.A. (2008): “Internet Banking Versus Other Banking Channels: Young Consumers’ View. International Journal of Information Management, Vol. 28, No: 3, pp. 215-221

Cole, S., (2000): “Myth of fingerprints: A forensic science stands trial” Lingua Franca 10(8), 54-62

Coventry, L., Angeli, A.D., and Johnson G., (2003) “Usability and Biometric Verification ad the ATM interface.” Proceedings of the SICHI conference on human factors in computing systems. New York, NY: ACM Press, 153-160

Biometric Technology Today (2005): “Financial success for biometrics?” Biometric Technology Today, Volume 13, Issue 4, April 2005, Pages 9–11. Available online: http://dx.doi.org/10.1016/S0969-4765(05)70289-7 (last access on 27.11.2013)

Biometric Technology Today (2010): “First biometric ATMs roll out in Poland” Biometric Technology Today, Volume 2010, Issue 6, June 2010 Pages 5,12

Bygrave, L.A. (2010): “Privacy and Data Protection in International Perspective” Stockholm Institute for Scandinavian Law & Lee A Bygrave ISSN 0085-5944. *56*, pp 165- 200

Dapp, T, F. (2012): “Homo biometricus: Biometric recognition systems and mobile internet services” Deutche Bank Research. Available online: http://20.fi/11332 (last access on 20.11.2013)

Financial Crimes Enforcement Network (FinCen) (2000): “A Survey of Electronic Cash, Electronic Banking and Internet Gaming” U.S: Deparment of the Treasury 2000. Available online: http://fincen.gov/news_room/rp/files/e-cash.pdf (last access on 23.10.2013)

Grijpink, J. (2001): “ Privacy Law: Biometrics and Privacy” Computer Law & Security Report, Vol. 17 no 3 2001

Grijpink, J., (2005): “Biometrics and Identity Fraud Protection, Two Barriers to Realizing the Benefits of Biometrics – A Chain Perspective on Biometrics, and Identity Fraud” Computer Law & Security Report 2005 21, 138-145

Gross, H., (1967): “The Concept of Privacy” New York University Law Review 42 N.Y.U.L Rev. (1967)

Hartung, D. (2012): “Vascular Pattern Recognition And its Application in Privacy-Preserving Biometric Online-Banking Systems” Doctoral Dissertations at Faculty of Computer Science and Media Technology at Gjovik University College 2-2012

Hazarika, P., Jickells S.M., Wolff, K., Russell, D.A (2010): “Muliplexed detection of metabolites of narcotic drugs from a single latent fingerprint" Analytical Chemistry, 2010, 82, 9150-9154

Hert, P.D. (2005): “Biometrics: Legal Issues and Implications, European Communities.” Available online: http://www.statewatch.org/news/2005/apr/jrc-biometrics-paul-de-hert.pdf (last access on 31.10.2013)

Hosseini, S.S. & Mohammadi, S. (2012): “ Review Banking on Biometric in the World’s Banks and Introducing a Biometric Model for Iran’s Banking System”. Journal of Basic and Applied Scientific Research. 2012 Textroad Publication

Kevenaar, T.A.M., Schrijen, G.J., van der Veen, M., Akkermans, A.H.M.,Zuo, F (2005) "Face Recognition with Renewable and Privacy Preserving Binary Templates," autoid, pp.21-26, Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05), 2005

Kinnunen, T., Wu, Z., Lee, K., Sedlak, F., Siong Chng, E., Li, H., (2012): ”Vulnerability of Speaker Verification Systems Against Voice Conversion Spoofing Attacks: the Case of Telephone Speech” in Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on. IEEE, 2012, pp. 4401-4404.

Konstari, T. (1992): “Henkilörekisterilaki. Säännökset ja käytäntö” Lakimiesliiton kustannus. Helsinki 1992

Kriikkula, A. (2006): “Biometriset tunnisteet ja tietosuoja erityisesti pankkialan sovelluksiin liittyen” Pro gradu- tutkielma 2006 University of Lapland

Lee, D.T (2004): “Re-examining the security issues of ATM systems” Computer Fraud & Security 2004 Elsevier, pp. 13-15

Liao, S., Pu Shao, Y., Wang, H., Chen, A. (1999): "The adoption of virtual banking: an empirical study" International Journal of Information Management 19 (1999) pp. 63-74

Liu, Y., (2010): "Bio-Privacy: Legal Challenges for Privacy Regulations of Biometric Identification and Authentication" Norwegian Research Center for Computers and Law, Institute of Private Law, Faculty of Law, University of Oslo. No. 35 March 2010

Lohiya, S. (2012): "Biometric Identification and Verification Techniques – A Future of ATM Banking System" Indian Streams Research Journal, Volume 2, Issue. 7, Aug 2010. Available online: http://www.isrj.net/UploadedData/1235.pdf (last access on 7.11.2013)

Margulis, S. (2011): "Three Theories of Privacy: An Overview" Privacy Online – Perspectives on Privacy and Self-Disclosure in the Social Web, Springer Berlin Heidelberg, pp, 9-17

McCoy, S. (2002) "O' big brother where art thou? The Constitutional Use of Facial-Recognition Technology" John Marshall Journal of Computer & International Law, XX(3), 471-485

Omariba, Z., Masese, N., Wanyembi, G., (2012): "Security and Privacy of Electronic Banking" International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012

Onyesolu, M.O. and Ezeani, M.I. (2012): "ATM Security Using Fingerprint Biometric Identifier. An Investigate Study" International Journal of Advanced Computer Science and Applications, 3(5), pp.67-74

Orr, B. & Bielski, L. (2000): "Time to start planning for biometrics", ABA Banking Journal. Oct. 2000, Vol.92 Issue 10, 3p. 1 Color Photograph

Reed, C. (2012): “Making Laws for Cyberspace” Oxford, Oxford University press 2012

Sarma, G. and Singh P,K. (2010): “Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication” International Journal of Pure and Applied Sciences and Technology ISSN 2229-6107 2010, pp-67-78

Scott, W. A. (1914): “Banking” Chicago A.C. McClurg & Co. 1914

Stoney, D.A. (1997): “Fingerprint identification: Scientific Status. In D.L. Faigman, D.H. Kaye, M.J. Saks & J. Sanders Modern scientific evidence: The law and science of expert testimony, 368-399. St Paul, Mn: West Publishing

Solove, D. (2004): “The Digital Person: Technology and Privacy in The Information Age” NYU Press 2004

Suomen virallinen tilasto (SVT) (2010): “Väestön tieto- ja viestintätekniikan käyttö” ISSN=2341-8699. 2010, 4. Tietoturvahuolet ja internetin käyttö . Helsinki: Tilastokeskus

The Department of Treasury (2005): “The use of Technology to Combat Identity Theft” Report on the Study Conducted Pursuant to Section 157 of the Fair and Accurate Credit Transactions Act of 2003, February 2005

Van der Ploeg, I., (2005): “The Machine- Readable Body. Essays on biometrics and the informalization of the body” Center for Public Innovation. Shaker Publishing 2005

von Graevenitz, G. A., (2007): “Biometric authentication in relation to payment systems and ATMs – A new approach for biometric verification using finger veins and the start of the proliferation of biometric incorporated ATMs” Datenschutz und Datensichereheit 31 (2007)

Wayman, J. (2001) “Fundamentals of biometric authentication technologies.” Int. J. Imaging and Graphics 1 (1), 2001

Wayman, J., Jain, A., Maltoni D., Maio, D., (2005): “Biometric Systems: Technology, Design and Performance Evaluatio” Springer 2005, Berlin

Watanabe, M., Endoh, T., Shiohara, M., Sasaki, S.,(2005). “Palm Vein Authentication Technology and its Applications” Proceedings of the Biometric Consortium Conference (Fujitsu Laboratories)

Westin, AF (1967): “Privacy and Freedom New York” Atheneum, 1967,

Wuolijoki, S. (2005): “Verkkopankkitoiminnan oikeudellinen sääntely” Lakimies 2/2005, s. 234-258

Yampolskiy, R.V. and Govindaraju, V. (2008) ‘Behavioural biometrics: a survey and classification’, Int. J. Biometrics, Vol. 1, No. 1, pp.81-113

Yang, Y-J. (1997): “The Security of Electronic Banking” Metzerott Rd.adelphi. Available online: http://csrc.nist.gov/nissc/1997/proceedings/041.pdf (last access on 24.10.2013)

Zegiorgis, S. (2002): “Biometric Technology Stomps Identity Theft” Part of the Information Security Reading Room. SANS Institute 2002. Available online: https://www.sans.org/reading-room/whitepapers/authentication/biometric-technology-stomps-identity-theft-126 (last access on 31.10.2013)

News, Presentations and Statistics Online:

Fujitsu (2012a): “Fujitsu Builds Japan's First Palm Vein Authentication System for ATMs” Available online: http://www.fujitsu.com/global/news/pr/archives/month/2012/20120926-01.html (last access on 28.10.2013)

Fujitsu (2012b): “Biometric Applications for Financial Markets” ATMIA Conference, Moscow April 2012. Available online: http://20.fi/11159 (last access on 29.10.2013)

Gunn, L. (2010): “Would you use biometric technology at an ATM?” 1 September 2010 Finextra. Available online: http://www.finextra.com/community/fullblog.aspx?id=4419 (last access on 7.11.2013)

Hudson, A. (2012): “UK company using voice biometric to conduct financial transactions on iPhone” SecureIDNews, 21 June, 2013. Available online: http://secureidnews.com/news-item/uk-company-using-voice-biometric-to-conduct-financial-transactions-on-iphone-2/ (last access on 29.10.2013)

Ollila, K. (2012): “Suomalaisiin verkkopankkeihin hyökättiin- tähän saakka on selvitty säikähdyksellä” Tietoviikko 1/2012. Available online: http://www.tietoviikko.fi/kaikki_uutiset/suomalaisiin%20verkkopankkeihin%20hyokattiin%20%20quottahan%20saakka%20on%20selvitty%20saikahdyksellaquot/a759674 (last access on 20.11.2013)

Pettersson Maria (2013): “Miksi asiakkaalle ei myönnetty verkkopannkitunnuksia?” Helsingin Sanomat. October 2013. Available online: http://www.hs.fi/kuluttaja/a1380515227270 (last access on 25.11.2013)

Police of Finland (2013): “Maksukorttirikollisuus on kasvava rikosilmiö” Available online: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/57AB59140EEDBC15C225799C002B56EA (last access on 4.11.2013)

Repo, M. (2013): “Verkkopankki on perusoikeus” Helsingin Sanomat October 2013. Available online: http://www.hs.fi/mielipide/a1380700093914 (last access on 24.11.2013)

Statistics Finland (2010): “Official Statistics of Finland: Tieto- ja viestintätekniikan käyttö 2010 – Internet vuorovaikutuksen välineenä” Tiede, teknologia ja tietoyhteiskunta 2010. Tilastokeskus. Available online: http://www.stat.fi/til/sutivi/2010/sutivi_2010_2010-10-26_fi.pdf (last access on 1.11.2013)

Statistics Finland (2013): “Official Statistics of Finland: Poliisin tietoon tullut rikollisuus” Oikeus 2013. Tilastokeskus. Available online: https://tilastokeskus.fi/til/polrik/2012/04/polrik_2012_04_2013-01-17_fi.pdf (last access on 4.11.2013)

SecurityInfoWatch.com (2007): “Facial Recognition Not Ready for Prime-Time in Online Banking” SecurityInfoWathc.com January 8, 2007 Available online: http://20.fi/11161 (last access on 29.10.2013)